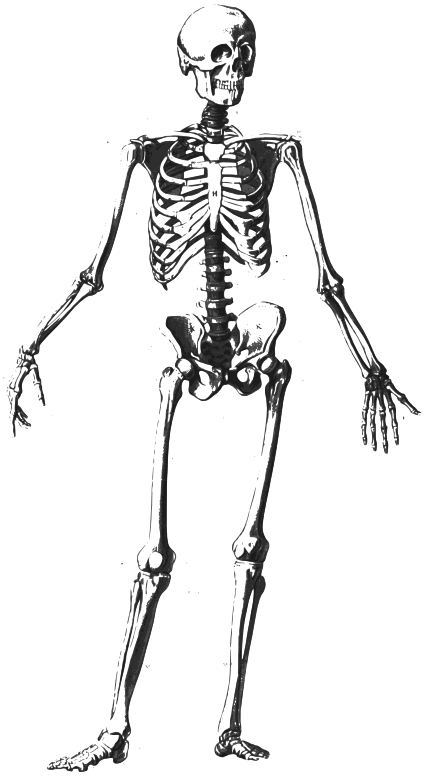
Math 581: Skeleton Notes



Bart Snapp

June 7, 2010

Chapter 1

Rings

Definition 1 *A **ring** is a set R with two operations: $+$ called addition and $\cdot$ called multiplication such that:*

(i) *$(R, +)$ is an abelian group with identity element denoted by 0.*

(ii) *Multiplication is associative:*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) *Multiplication distributes over addition:*

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{and} \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

(iv) *Multiplication is commutative:*

$$a \cdot b = b \cdot a$$

(v) *There is a multiplicative identity denoted by 1:*

$$a \cdot 1 = a$$

Remark *Depending on the source one reads, the definition of a ring might be restricted to items* (i)–(iii) *above. In that case, what is defined above would be called a commutative ring with identity. Henceforth when we write ring we mean a commutative ring with identity.*

1.1) Identify which of the following sets are rings. Give a careful explanation of why the set in question is a ring or is not a ring.

(i) The integers, $\mathbb{Z}$.

(ii) The even integers, $2\mathbb{Z} = \{2 \cdot n : n \in \mathbb{Z}\}$.

(iii) The odd integers.

(iv) The rational numbers, $\mathbb{Q}$.

(v) The integers modulo 2, $\mathbb{Z}_2$.

(vi) The integers modulo 6, $\mathbb{Z}_6$.

(vii) The positive rational numbers, $\mathbb{Q}^+$.

(viii) The real numbers, $\mathbb{R}$.

(ix) The polynomials with coefficients in $\mathbb{R}$ in one variable, $\mathbb{R}[x]$.

(x) The polynomials with coefficients in $\mathbb{R}$ in two variables, $\mathbb{R}[x, y]$.

(xi) The power series with coefficients in $\mathbb{R}$ in one variable, $\mathbb{R}[\![x]\!]$.

(xii) The set $\mathbb{Z} \times \mathbb{Q}$ where

$$(a, b) + (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$$

(xiii) Is the set of 2×2 matrices with entries in $\mathbb{Z}$ a noncommutative ring?

(xiv) The *Gaussian integers*,

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

(xv) The integers adjoin the square-root of 2,

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

(xvi) The set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

1.2) Prove the following basic facts about rings:

(i) $a \cdot 0 = 0$ and $0 \cdot a = 0$. Hint: Start with $a \cdot 0 = a \cdot (0 + 0)$.

(ii) $a \cdot (-b) = -(a \cdot b)$ and $(-a) \cdot b = -(a \cdot b)$.

(iii) $(-a)(-b) = ab$.

1.3) In each case, prove that the set of integers $\mathbb{Z}$ is a ring when "addition" is defined by $\maltese$ and "multiplication" is defined by $\star$:

(i) $a \maltese b = a + b - 1$ and $a \star b = ab - (a + b) + 2$.

(ii) $a \maltese b = a + b + 1$ and $a \star b = ab + a + b$.

1.4) Given any two rings R and S, prove that $R \times S$ is a ring where

$$(a, b) + (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$$

The ring $R \times S$ with this "addition" and "multiplication" is called the **direct product ring** of R and S. Note, sometimes this is written $R \oplus S$.

1.5) Prove that the set of ordered pairs in $\mathbb{Z} \times \mathbb{Z}$ is a ring when "addition" is defined by $\maltese$ and "multiplication" is defined by $\star$:

$$(a, b) \maltese (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \star (c, d) = (ac - bd, ad + bc).$$

Definition 2 *A **field** $(F, +, \cdot)$ is a commutative ring with identity along with the condition that $F - \{0\}$ is also an abelian group under multiplication.*

2.1) Write out all the specific conditions that are necessary for F to be a field.

2.2) Draw a Venn diagram showing the relationship between groups, rings, and fields. Be very careful about specifying the relevant operations. Give relevant and revealing examples for each section of the diagram.

2.3) Let a and b be elements of a field F. Prove that if $a \cdot b = 0$, then a is zero or b is zero. Is the same statement true for rings in general? If so, give a proof. If not, give a counterexample.

2.4) When is $\mathbb{Z}_n$ definitely not a field?

2.5*) Describe a field with four elements.

2.6*) Can you find a field with six elements?

2.7) Let F be a field. Find some quality inherent in F that is necessary and sufficient to make the set of ordered pairs in $F \times F$ a field when "addition" is defined by $\maltese$ and "multiplication" is defined by $\star$:

$$(a, b) \maltese (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \star (c, d) = (ac - bd, ad + bc).$$

Hint: What if $F = \mathbb{R}$? What if $F = \mathbb{C}$? Keep on going!

Definition 3 *Given a ring R, a **unit** is an element u such that there exists an element v with $u \cdot v = 1$.*

3.1) List the units in the following rings:

(i) $\mathbb{Z}$

(ii) $\mathbb{Q}$

(iii) $\mathbb{C}$

(iv) $\mathbb{Z}_5$

(v) $\mathbb{Z}_6$

(vi) Give a conjecture for the units in $\mathbb{Z}_n$

3.2) Prove that if u is a unit and v is a unit, then $u \cdot v$ is a unit.

3.3) Give an example of a ring with a unit a such that $a^2 = 1$ and $a \neq \pm 1$.

3.4) Prove that if $a \neq \pm 1$ and $a^2 = 1$, then $(a+1)(a-1) = 0$.

Definition 4 *A **zero-divisor** is a nonzero element in a ring $z \in R$ such that there is some nonzero $a \in R$ with*

$$a \cdot z = 0.$$

4.1) Prove that a field cannot contain zero-divisors.

4.2) Prove that if ab is a zero-divisor then either a is a zero-divisor or b is a zero-divisor.

4.3) Can a zero-divisor have a multiplicative inverse? Prove your conclusion.

4.4) If $z^2 = 0$, prove that $z+1$ and $z-1$ are invertible. Give an example of a ring R and an element z where this is the case.

4.5) Let R and S be rings. Prove that the direct product ring $R \times S$ always will have zero-divisors. See (1.4).

Definition 5 *An **integral domain**, often called a **domain**, is a ring containing no zero-divisors.*

5.1) Prove that the following are equivalent:

(i) R is an integral domain.

(ii) For $a, b \in R$ if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

(iii) For $a, b, c \in R$ if $a \neq 0$, then

$$ab = ac \qquad \Rightarrow \qquad b = c.$$

(iv) $R - \{0\}$ is closed under multiplication.

Remark *Property* (iii) *above is called the **cancellation** property of domains.*

5.2) Prove that a field is an integral domain.

5.3) Give examples of integral domains along with examples of rings that are not integral domains.

5.4) Draw a Venn diagram showing the relationship between rings, integral domains, and fields. Be very careful about specifying the relevant operations. Give relevant and revealing examples for each section of the diagram.

5.5) Explain why $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{3}]$, and $\mathbb{Z}[\sqrt{-5}]$ are all integral domains.

5.6) Let R be an integral domain and consider a nonzero element $a \in R$. Define a map $\varphi : R \to R$ such that:

$$x \mapsto ax$$

Prove that φ is an injection.

Theorem 5.7 *Every finite integral domain is a field.*

Sketch of Proof Let R be the finite integral domain and consider any nonzero element $a \in R$. Now consider the set $\{a^n : n \in \mathbb{N}\}$. ■

5.8) Given a finite field, give a basic strategy for finding a multiplicative inverse of an element.

Definition 6 *Given a ring R with $n, d \in R$, we say d **divides** n, denoted $d|n$, if*

$$n = dq$$

where $q \in R$. What do we write if d does not divide n?

6.1) Prove the following:

(i) If $a|b$ and $b|c$, then $a|c$.

(ii) $a|b$ if and only if $a|(-b)$.

(iii) $a|0$.

Definition *A nonzero element p of a ring R is called **prime** if it is not a unit and*

$$p|ab \qquad \Rightarrow \qquad p|a \text{ or } p|b$$

for all $a, b \in R$.

*A nonzero element p of a ring R is called **irreducible** if it not a unit and*

$$p = a \cdot b \qquad \Rightarrow \qquad a \text{ or } b \text{ is a unit}$$

for all $a, b \in R$.

6.2) What does it mean to say an element n is not prime?

6.3) If R is a domain, prove that every prime element is irreducible. Hint, if $p = ab$, then $p|ab$ (why?).

6.4*) Are prime elements always irreducible?

6.5*) Are irreducible elements always prime?

6.6) Prove or disprove: Given $a, b \in \mathbb{Z}$

$$a|b^n \Rightarrow a|b$$

where $n \in \mathbb{N}$. What can you say if a is prime?

6.7) Given a prime p, prove that $\mathbb{Z}_p$ is an integral domain. Use (5.7) to conclude that $\mathbb{Z}_p$ is a finite field. Note, this is an *indirect* proof. While we show that inverses to nonzero elements exist, we give no hint as how to actually find them! Can you think of a direct proof of the fact that $\mathbb{Z}_p$ is a field?

Definition 7 *The **characteristic** of a ring R is the least positive integer n such that*

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0.$$

If there is no such positive integer, then we say that R has characteristic 0.

7.1) Prove that if an integral domain has a finite characteristic, then its characteristic is a prime number.

7.2) Prove that in a domain of positive characteristic p, the so-called *Freshman Binomial Theorem* holds:

$$(a+b)^p = a^p + b^p$$

Definition 8 *A **polynomial ring** $R[x]$ is the set of all formal sums*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where n is a nonnegative integer and each $a_i \in R$.

8.1) Perform the following computations in $\mathbb{Z}[x]$, $\mathbb{Z}_3[x]$, and in $\mathbb{Z}_2[x]$:

(i) $x + x$

(ii) $(x+1)(x+1)$

(iii) $(x+1)^3$

8.2) Let R be an integral domain. Prove that $R[x]$ is an integral domain.

8.3) Let R be an integral domain and let $p(x)$ and $q(x)$ be nonzero elements of $R[x]$. Prove that

$$\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x)).$$

Is this result necessarily true if R is not an integral domain? Give a proof or counterexample to justify your claim.

8.4) Let R be an integral domain. Prove that the units of $R[x]$ are exactly the units of R.

8.5) Describe an infinite integral domain of characteristic p.

Theorem 9 *Every finite field has order p^n for some prime p and some natural number n.*

Sketch of Proof Consider a finite field F.

(i) Explain why F must have finite prime characteristic.

(ii) Explain why the set

$$k = \left\{ \sum_{i=1}^{n} 1 : n \in \mathbb{N} \right\} \subseteq F$$

is an integral domain of prime order. Conclude that k is a finite field, see (5.7).

(iii) Prove that F is a k-vector space. You may need to refer to your linear algebra text for help!

(iv) Explain why F is a finite dimensional vector space over k.

(v) If the dimension of F over k is 1, how many elements does F have? What if the dimension is 2? What if the dimension is n?

(vi) Use the steps above to explain why every finite field has order p^n for some prime p and some natural number n.

Note, this is a *non-constructive* proof. While we show that finite fields have order p^n, see (2.6), we give no indication as how to actually find finite fields of order p^n. At this point, for some values of p and n these objects may not even exist! Can you think of a way to construct fields of order p^n? ■

9.1) Prove that $\mathbb{Z}_3[i]$ is a finite field. How many elements does it have?

9.2) Prove that $\mathbb{Z}_7[\sqrt[3]{2}]$ is a finite field. How many elements does it have?

Chapter 2

Division

Definition 10 *Given a ring R, an **ideal** I of R is an additive subgroup of R where the following condition holds:*

$$x \in R \text{ and } a \in I \Rightarrow x \cdot a \in I$$

10.1) Prove that the set $\{0\}$ is always an ideal.

10.2) Prove that every ideal contains zero.

10.3) Let R be a ring and I be an ideal of R. Prove that if $1 \in I$, then $I = R$.

10.4) Prove that a ring R is a field if and only if the only ideals of R are $\{0\}$ and R.

10.5) Identify which of the following sets are ideals. Give a careful explanation of why the set in question is an ideal or is not an ideal.

(i) $4\mathbb{Z} = \{4n : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$

(ii) $(8\mathbb{Z} \cap 12\mathbb{Z}) \subseteq \mathbb{Z}$

(iii) The subset of $\mathbb{Z}[x]$ consisting of the set of polynomials whose constant term is a multiple of 7.

(iv) The subset of $\mathbb{Z}[x]$ consisting of the set of polynomials whose x^2 is a multiple of 7.

(v) The subset of $\mathbb{Z}[x]$ consisting of the set of polynomials consisting only of even degree terms.

(vi) The subset of $\mathbb{Z}[x]$ consisting of the set of polynomials with no terms of degree less than 4.

(vii) The subset of $\mathbb{Z}[x]$ consisting of the set of polynomials whose coefficients sum to zero.

(viii) The subset of $\mathbb{Z}[x]$ consisting of the set of polynomials whose first derivative with respect to x is zero when evaluated at zero.

(ix) $\{(n, n) : n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$

(x) $\{(7n, 0) : n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$

(xi) $\{(m, n) : m + n \text{ is even}\} \subseteq \mathbb{Z} \times \mathbb{Z}$

(xii) $\{(2m, 3n) : m, n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$

10.6) List all the ideals of $\mathbb{Z}_{12}$.

10.7) List all the ideals of $\mathbb{Z}_3 \times \mathbb{Z}_3$.

10.8) Let $\ell = \{(a, b) \in \mathbb{R}^2 : 3a + 2b = 4\}$ be a line in $\mathbb{R}^2$. Prove that

$$I = \{f(x, y) \in \mathbb{R}[x, y] : f(a, b) = 0 \text{ for all } (a, b) \in \ell\}$$

is an ideal of $\mathbb{R}[x, y]$.

10.9) Let $S^2 = \{(a, b, c) \in \mathbb{R}^3 : a^2 + b^2 + c^2 = 1\}$ be the unit sphere in $\mathbb{R}^3$. Prove that

$$I = \{f(x, y, z) \in \mathbb{R}[x, y, z] : f(a, b, c) = 0 \text{ for all } (a, b, c) \in S^2\}$$

is an ideal of $\mathbb{R}[x, y, z]$.

10.10) Let I and J be ideals of R.

(i) Prove that $I + J = \{a + b : a \in I \text{ and } b \in J\}$ is an ideal of R.

(ii) Prove that $IJ = \{\sum a_i b_j : a_i \in I \text{ and } b_j \in J\}$ is an ideal of R.

(iii) Prove that $I \cap J$ is an ideal of R.

10.11) Find a ring R along with two ideals I and J such that $I \cup J$ is **not** an ideal of R.

10.12) Summarize the conclusions of (10.10) and (10.11).

10.13) Let I and J be ideals of R. Prove that:

$$IJ \subseteq (I \cap J)$$

Give an example of where $IJ \neq (I \cap J)$.

10.14*) For $m, n \in \mathbb{Z}$, when is it the case that

$$(m \cdot n)\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}?$$

10.15) Given a ring R, if $a \in R$, we write (a) to denote the smallest ideal of R containing a. On the other hand, we write aR to denote all the multiples of a. Prove that:

$$(a) = \{ar : r \in R\} = aR$$

10.16) Given a ring R, if $X \subseteq R$, we write (X) to denote the smallest ideal of R containing the subset X. Prove that

$$(X) = \left\{ \sum_{i=1}^{n} a_i r_i : r_i \in R, a_i \in X, \text{ and } n \text{ is some nonnegative integer} \right\}.$$

We call X a **generating set** for the ideal. Note, X could be infinite!

10.17) An ideal I is called a **principal ideal** if it is generated by a single element. Prove that the following ideals are principal ideals:

(i) $(3, 6, 9) \subseteq \mathbb{Z}$

(ii) $(-18, 9) \subseteq \mathbb{Z}$

(iii) $\mathbb{Z}$ as an ideal of $\mathbb{Z}$

(iv) $(2, 3) \subseteq \mathbb{Z}$

(v) $(12, 18) \subseteq \mathbb{Z}$

10.18) Can you think of a ring with an ideal that is not principal?

10.19) Consider $f, g \in R[x]$ where R is a domain.

(i) Prove that given two polynomials f and g

$$\deg(f+g) \leqslant \max\{\deg(f), \deg(g)\} \qquad \text{and} \qquad \deg(f \cdot g) = \deg(f) + \deg(g).$$

(ii) Prove or disprove: The ideal $(2, x)$ is not principal in $\mathbb{Z}[x]$.

(iii) Prove or disprove: The ideal $(2, x)$ is not principal in $F[x]$ where F is a field.

Theorem 11 (Division Theorem) *Given any integer n and a nonzero integer d, there exist unique integers q and r such that*

The above space has intentionally been left blank for you to fill in. Remember with division we are trying to fill in the following diagram:

$$\begin{array}{r} q \text{ R} r \\ d\overline{)n} \end{array} \qquad \text{where} \qquad \begin{array}{l} d \text{ is the divisor} \\ n \text{ is the dividend} \\ q \text{ is the quotient} \\ r \text{ is the remainder} \end{array}$$

11.1) How do you know when integers n, d, q, and r satisfy the above property? Write this into the Division Theorem above.

11.2) We will prove that the quotient and remainder in the Division Theorem are unique.

(i) Suppose that (q_1, r_1) and (q_2, r_2) both satisfied the conditions of the Division Theorem for a divisor n and dividend d. Use these two equations to produce a third equation relating d, q_1, q_2, r_1, and r_2.

(ii) If $q_1 \neq q_2$ explain why $|r_1 - r_2| \geqslant |d|$.

(iii) Prove uniqueness of the quotient and remainder in the Division Theorem.

11.3) We will prove that the quotient and remainder in the Division Theorem exist.

(i) Prove the existence of q and r if $n = 0$.

(ii) Prove the existence of q and r if $d|n$.

(iii) Suppose that $n \neq 0$ and $d \nmid n$. Consider the set:

$$S = \{n - dk : k \in \mathbb{Z}\} \cap \mathbb{N}$$

Explain why S is not empty.

(iv) Explain why S has a least element.

(v) Call the least element found above r, explain why $r < |d|$.

(vi) Explain how to choose q satisfying the conditions of the Division Theorem.

11.4) Using our work above, write a complete proof of the Division Theorem.

11.5) Formulate and prove a version of the Division Theorem for integers allowing negative remainders. Will you be able to preserve uniqueness of the quotient and remainder? Give a proof or counterexample.

Definition 12 *Given a ring R, g is called a* ***greatest common divisor*** *of two elements a and b provided that*

(i) *$g|a$ and $g|b$.*

(ii) *If d is an element where $d|a$ and $d|b$, then $d|g$.*

12.1) Given $n \in \mathbb{Z}$, what is $(n, 0)$? Prove your conclusion.

12.2) Prove that if n is any integer, then $(a + n \cdot b, b) = (a, b)$.

12.3) If $g = (a, b)$ and u is a unit, prove that gu is also a greatest common divisor of a and b.

12.4) Given nonzero $a, b \in \mathbb{Z}$, we will prove that $g = (a, b)$ is the *smallest* positive integer such that

$$g = a \cdot m + b \cdot n$$

for some integers m and n.

(i) Let $S = \{x \in \mathbb{N} : x = a \cdot m + b \cdot n \text{ for } m, n \in \mathbb{Z}\}$. Prove that S has a least element, call it d.

(ii) Prove that $d|x$ for all $x \in S$.

(iii) Prove that $d|a$ and $d|b$, explain why $1 \leqslant d \leqslant g$.

(iv) Recall that $d = a \cdot m + b \cdot n$, and prove that $g|d$. Explain why we must conclude that $d = g$.

12.5) Let a, b, and c be nonzero integers. Suppose that

$$a|bc \qquad \text{and} \qquad (a, b) = 1.$$

Prove that $a|c$.

12.6) We will prove that in the integers, all irreducible elements are prime, see (6.5). Let p be irreducible and let $a, b \in \mathbb{Z}$ such that $p|ab$.

(i) Suppose that $p \nmid a$, explain why $(a, p) = 1$.

(ii) Write $1 = am + pn$, multiply both sides by b.

(iii) Can you finish it from here?

Remark *The statements of (12.4), (12.5), and (12.6) are all sometimes referred to as* ***Euclid's Lemma****.*

12.7) Prove that if $(m, n) = 1$, then

$$in \equiv jn \pmod{m} \qquad \Rightarrow \qquad i \equiv j \pmod{m}.$$

Theorem 12.8 (Euclidean Algorithm) *We can easily compute the GCD of two numbers using the following algorithm:*

The above space has intentionally been left blank for you to fill in.

12.9) Study the following calculations:

$$\begin{aligned} 22 &= \mathbf{6} \cdot 3 + \mathbf{4} \\ 6 &= \mathbf{4} \cdot 1 + \boxed{\mathbf{2}} \\ 4 &= 2 \cdot 2 + 0 \qquad \therefore (22, 6) = 2 \end{aligned}$$

$$\begin{aligned} 33 &= \mathbf{24} \cdot 1 + \mathbf{9} \\ 24 &= \mathbf{9} \cdot 2 + \mathbf{6} \\ 9 &= \mathbf{6} \cdot 1 + \boxed{\mathbf{3}} \\ 6 &= 3 \cdot 2 + 0 \qquad \therefore (33, 24) = 3 \end{aligned}$$

$$\begin{aligned} 42 &= \mathbf{16} \cdot 2 + \mathbf{10} \\ 16 &= \mathbf{10} \cdot 1 + \mathbf{6} \\ 10 &= \mathbf{6} \cdot 1 + \mathbf{4} \\ 6 &= \mathbf{4} \cdot 1 + \boxed{\mathbf{2}} \\ 4 &= 2 \cdot 2 + 0 \qquad \therefore (42, 16) = 2 \end{aligned}$$

Explain how the above algorithm works and write it under the Euclidean Algorithm above.

12.10) We will prove that when working with integers, the Euclidean Algorithm will always produce the GCD of two numbers.

(i) Prove that the remainders found in the Euclidean Algorithm form a decreasing sequence.

(ii) Prove that this sequence must terminate with a final remainder of zero.

(iii) Proceed by induction on the number of steps in the Euclidean Algorithm. If there are two steps:

$$\begin{aligned} a &= b \cdot q_1 + g \\ b &= g \cdot q_2 + 0 \end{aligned}$$

Prove that any divisor of both a and b is necessarily a divisor of g. Explain why this proves that $g = (a, b)$.

(iv) Now suppose that any time we have $n+1$ equations:

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n \\ r_{n-1} &= r_n \cdot q_{n+1} + 0 \end{aligned}$$

that $r_n = (a, b)$. Prove that when we have $n+2$ equations, $r_{n+1} = (a, b)$.

(v) Explain how we have proved that when working with integers, the Euclidean Algorithm will always produce the GCD of two numbers.

12.11) Prove that if $x = am + bn$ and d is a common divisor of a and b, then $d|x$. What does this say about the GCD of a and b?

12.12) Each of the following ideals of $\mathbb{Z}$ is principal, use the Euclidean algorithm to find the generator.

(i) $(12, 16) \subseteq \mathbb{Z}$

(ii) $(12, 17) \subseteq \mathbb{Z}$

(iii) $(12, 18) \subseteq \mathbb{Z}$

(iv) $(12, 16, 24) \subseteq \mathbb{Z}$

(v) $(12, 16, 24, 35) \subseteq \mathbb{Z}$

12.13) Explain why the notation (a, b) for the GCD of a and b along with the notation (a, b) for the ideal generated by a and b is not confusing at all.

12.14) Prove that for $m, n \in \mathbb{Z}$ if $(m, n) = 1$, then

$$(m \cdot n)\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}.$$

See (10.13) and (10.14).

Definition 13 *A **Diophantine equation** is an equation where one insists that the solutions are integers.*

13.1) Study the following calculations:

$$\begin{array}{rcl} 22 = 6 \cdot 3 + 4 & \Leftrightarrow & 22 - 6 \cdot 3 = \mathbf{4} \\ 6 = 4 \cdot 1 + 2 & \Leftrightarrow & 6 - \mathbf{4} \cdot 1 = 2 \\ 4 = 2 \cdot 2 + 0 & & \end{array} \qquad \begin{array}{r} 6 - 4 \cdot 1 = 2 \\ 6 - (22 - 6 \cdot 3) \cdot 1 = 2 \\ 6 \cdot 4 + 22(-1) = 2 \end{array}$$

$$
\begin{aligned}
33 &= 24 \cdot 1 + 9 &\Leftrightarrow\quad 33 - 24 \cdot 1 &= \mathbf{9} \\
24 &= 9 \cdot 2 + 6 &\Leftrightarrow\quad 24 - \mathbf{9} \cdot 2 &= \mathbf{6} \\
9 &= 6 \cdot 1 + 3 &\Leftrightarrow\quad 9 - \mathbf{6} \cdot 1 &= 3 \\
6 &= 3 \cdot 2 + 0
\end{aligned}
$$

$$
\begin{aligned}
9 - 6 \cdot 1 &= 3 \\
9 - (24 - 9 \cdot 2) \cdot 1 &= 3 \\
9 \cdot 3 + 24 \cdot (-1) &= 3 \\
(33 - 24 \cdot 1) \cdot 3 + 24 \cdot (-1) &= 3 \\
33 \cdot 3 + 24 \cdot (-4) &= 3
\end{aligned}
$$

Explain how to solve Diophantine equations of the form

$$ax + by = g$$

where $g = (a, b)$.

13.2) For each of the following Diophantine equations, give a solution or explain why no solution exists.

(i) $20x + 13y = 1$

(ii) $20x + 13y = 2$

(iii) $18x + 17y = 5$

(iv) $18x + 22y = 14$

(v) $18x + 22y = 5$

13.3) Explain how to solve Diophantine equations of the form

$$ax + by = c.$$

Also explain how to identify when such an equation has no solution.

13.4) We will construct multiplicative inverses in $\mathbb{Z}_p$.

(i) Consider $x \in \mathbb{Z}_p$ where $x \neq 0$. Explain why $(x, p) = 1$.

(ii) Use (12.4) to give an equation relating x and p.

(iii) Explain how you have found an inverse for x in $\mathbb{Z}_p$.

13.5) Find the following ring elements:

(i) Find the multiplicative inverse of 9 in $\mathbb{Z}_{11}$.

(ii) Find the multiplicative inverse of 5 in $\mathbb{Z}_{13}$.

(iii) Find the multiplicative inverse of 7 in $\mathbb{Z}_{17}$.

(iv) Find the multiplicative inverse of 5 in $\mathbb{Z}_{12}$.

(v) Find the multiplicative inverse of 7 in $\mathbb{Z}_{24}$.

13.6) Given an integer n, explain which elements in $\mathbb{Z}_n$ have multiplicative inverses.

Definition 14 *An integral domain where every ideal is principal is called a* ***principal ideal domain*** *or a PID.*

14.1) We will prove that $\mathbb{Z}$ is a principal ideal domain.

(i) Explain why an ideal $I \subseteq \mathbb{Z}$ has a least positive element.

(ii) Call the least positive element found above $a \in I$. Explain why a necessarily divides any other element of I.

(iii) Explain why $(a) = I$.

14.2) Give some examples of PID's and also give some nonexamples of PID's.

14.3) Write down an ideal of $\mathbb{Z}$ generated by an infinite number of elements. Explain how you know that one element will suffice to generate this ideal.

14.4) Compare/contrast the methods used to solve (12.12) and (14.1).

14.5) What properties of the integers are needed to ensure that the technique of (14.1) will produce a principal ideal?

14.6) Prove that if R is a PID, then all irreducible elements are prime, see (6.5). Hint, see (12.6).

Definition 15 *An integral domain R is called a* ***euclidean domain*** *if there is a function $d : R - \{0\} \to \mathbb{N}$ such that*

(i) *For all nonzero a and b, $d(a) \leqslant d(ab)$.*

(ii) *For all $a, b \in R$ with $b \neq 0$, we can find q and r in R such that*

$$a = bq + r, \qquad d(r) < d(b) \text{ or } r = 0.$$

Theorem 15.1 *Prove that every euclidean domain is a PID.*

Sketch of Proof See (14.1). ■

Theorem 15.2 (Polynomial Division Theorem) *Let F be a field and consider any polynomial $n(x) \in F[x]$ and a nonzero polynomial $d(x)$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that*

$$n(x) = d(x)q(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } \deg(r) < \deg(d).$$

15.3) Prove that the quotient and remainder in the Polynomial Division Theorem are unique.

(i) Suppose that (q_1, r_1) and (q_2, r_2) both satisfied the conditions of the theorem for a divisor $n(x)$ and dividend $d(x)$. Use these two equations to produce a third equation relating d, q_1, q_2, r_1, and r_2.

(ii) If $q_1 \neq q_2$ explain why $\deg(r_1 - r_2) \geqslant \deg(d)$.

(iii) Prove uniqueness of the quotient and remainder in the Polynomial Division Theorem.

15.4) We will prove that the quotient and remainder in the Polynomial Division Theorem exist.

(i) Prove the existence of $q(x)$ and $r(x)$ if $\deg(n(x)) = 0$.

(ii) Prove the existence of $q(x)$ and $r(x)$ if $d(x)|n(x)$.

(iii) Suppose that $\deg(n(x)) \neq 0$ and $d(x) \nmid n(x)$. Consider the set:

$$S = \{1 + \deg(n(x) - d(x)k(x)) : k(x) \in F[x]\}$$

Explain why S is not empty.

(iv) Explain why S has a least element.

(v) Use the least element found above to obtain an element $r(x)$ and explain why $\deg(r) < \deg(d)$. Hint, suppose that $\deg(r) \geqslant \deg(d)$ and consider the polynomial

$$s(x) = r(x) - cx^{\deg(r)-\deg(d)} \cdot d(x)$$

for some suitable value of c.

(vi) Explain how to choose $q(x)$ satisfying the conditions of the Polynomial Division Theorem.

15.5) Explain why a polynomial ring over a field in a single variable is a euclidean domain.

15.6) Is $\mathbb{Z}[x]$ a euclidean domain? Prove your claim.

15.7) Is $F[x, y]$ a euclidean domain? Prove your claim.

15.8) Prove that the polynomial $x^n - 1 \in \mathbb{Q}[x]$ is divisible by the polynomial $x^m - 1$ if and only if $m|n$.

15.9) Factor the polynomials $x - 1, x^2 - 1, x^3 - 1, \ldots, x^{12} - 1$ into as many factors with rational coefficients as possible. Can you find a pattern? Can you predict the number of irreducible factors of $x^n - 1$ in $\mathbb{Q}[x]$?

15.10) We will prove that the ring of Gaussian integers $\mathbb{Z}[i]$ is a euclidean domain and hence is a PID.

(i) Very briefly explain why the Gaussian integers are a domain.

(ii) Prove that $d(a+bi) = a^2+b^2$ satisfies (i) from the definition of a euclidean domain.

(iii) To see (ii) from the definition of a euclidean domain, we wish to show that given $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exists γ and ρ such that

$$\alpha = \beta\gamma + \rho, \qquad \text{where } d(\rho) < d(\beta) \text{ or } \rho = 0.$$

(iv) Prove the existence of γ and ρ if $\alpha = 0$.

(v) Prove the existence of γ and ρ if $\beta = \pm 1, \pm i$.

(vi) Suppose that $\alpha \neq 0$ and $d(\beta) > 1$. Consider the set:

$$S = \{d(\alpha - \beta\delta) : \delta \in \mathbb{Z}[i]\}$$

Explain why S is not empty.

(vii) Explain why S has a least element. Use this element to produce an element in $\mathbb{Z}[i]$, call it ρ.

(viii) If you plot β in the complex plane, explain why i is merely a 90° counter-clockwise rotation.

(ix) Noting that

$$\beta \cdot (a + bi) = \underbrace{\beta \cdot a}_{\text{scales by } \alpha} + \underbrace{\beta \cdot bi}_{\substack{\text{rotates } 90^\circ \\ \text{and scales by } b}}$$

draw a lattice in the complex plane representing complex multiples of β.

(x) Explain why $d(\rho) < d(\beta)$ and how to choose γ.

15.11) Prove that $\mathbb{Z}[\omega]$ is a euclidean domain where

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$$

and $d(a + b\omega) = a^2 - ab + b^2$. Hint, see (15.10) and think about the following elementary claim from geometry: Given a rhombus of side length a, any point in the rhombus is at most of distance a from any corner.

15.12) Prove that a PID will satisfy the *ascending chain condition* (ACC) on ideals: Given any ascending chain of ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

there exists a value m such that

$$I_m = I_{m+1} = I_{m+2} = \cdots$$

15.13) Explain factorization of integers in terms of ascending chains of ideals.

15.14) Each of the following ideals of $\mathbb{Z}_2[x]$ is principal, use the Euclidean algorithm to find the generator.

(i) $(x^2+1, x^2+x) \subseteq \mathbb{Z}_2[x]$

(ii) $(x^3+x, x^2+x) \subseteq \mathbb{Z}_2[x]$

(iii) $(x^3+x+1, x^2+x) \subseteq \mathbb{Z}_2[x]$

(iv) $(x^5+x^2+x, x^4+x, x^3+x^2) \subseteq \mathbb{Z}_2[x]$

15.15*) Are there principal ideal domains that are not euclidean domains?

15.16) Given any euclidean domain R, prove Euclid's Lemma (all three forms) for R. See (12.4), (12.5), and (12.6).

15.17) Draw a Venn diagram showing the relationship between rings, integral domains, fields, principal ideal domains, and euclidean domains. Give relevant and revealing examples for each section of the diagram. You might need to leave some "mystery" in your diagram!

Definition 16 *An integral domain R is called a **unique factorization domain** (or UFD) if every nonzero, nonunit element $x \in R$ has the following two properties:*

(i) *x can be written as a finite product of irreducible elements.*

(ii) *The product is unique up to order and multiplication by units.*

16.1) Explain why every field is a UFD.

16.2) We will show that every nonunit integer has a factorization into irreducible elements. Let B be the set of integers whose absolute value is greater than 1 that *do not* factor into irreducible elements.

(i) How do we know that B has a least element ℓ?

(ii) Explain why ℓ is not irreducible.

(iii) Explain why $\ell = m \cdot n$ where $m, n < \ell$.

(iv) What can you conclude about m and n? What does this say about ℓ?

16.3) We will show that if a nonunit integer has a factorization into irreducible elements, then this factorization is unique up to ordering and units.

(i) Let n be the number with the smallest absolute value such that it has two distinct factorizations into units u, v, and irreducibles:

$$n = u \cdot p_1 \cdot p_2 \cdots p_r = v \cdot q_1 \cdot q_2 \cdots q_s$$

By Euclid's Lemma (12.6), we have that $p_1 | q_1 q_2 \cdots q_s$ implies that $p_1 | q_i$ for some i. Hence $p_1 = q_i$.

(ii) Finish the proof.

Remark *Exercises (16.2) and (16.3) prove that $\mathbb{Z}$ is a UFD. If we restrict ourselves to the natural numbers, then we can avoid the issue with units. The theorem that states that factorization is unique in the natural numbers is called the* ***Fundamental Theorem of Arithmetic****.*

Theorem 16.4* *Every PID is a UFD.*

Corollary *Every euclidean domain is a UFD.*

16.5) Factor $x^4 + 1$ in $\mathbb{Z}[i]$ and in $\mathbb{Z}[\sqrt{2}]$. Note, both rings are UFD's.

16.6) We will show that in $R = \mathbb{Z}[\sqrt{-5}]$, some numbers can factor into irreducible elements in two different ways.

(i) Define a function

$$\begin{aligned} N : R - \{0\} &\to \mathbb{N} \\ a + b\sqrt{-5} &\mapsto a^2 + 5b^2 \end{aligned}$$

Prove that $N(\alpha) \cdot N(\beta) = N(\alpha\beta)$.

(ii) Prove that μ is a unit in R if and only if $N(\mu) = 1$.

(iii) Prove that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible in R.

(iv) Find two distinct factorizations of 6 into irreducible elements in R.

(v) Could it be the case that there are units $u, v \in \mathbb{Z}[\sqrt{-5}]$ with $u \cdot 2 = 1 \pm \sqrt{-5}$ and $v \cdot 3 = 1 \mp \sqrt{-5}$?

Explain why $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, and hence not a euclidean domain.

16.7) Draw a Venn diagram showing the relationship between rings, integral domains, fields, principal ideal domains, euclidean domains, and unique factorization domains. Give relevant and revealing examples for each section of the diagram. You might need to leave some "mystery" in your diagram!

Chapter 3

Quotient Rings and Homomorphisms

Definition 17 *Given a ring R and an ideal $I \subseteq R$, we can form a new ring called the* ***quotient ring*** *R/I. The elements of R/I consist of left additive cosets of I with addition and multiplication defined as follows:*

$$(a+I)+(b+I)=(a+b)+I$$
$$(a+I)\cdot(b+I)=(ab)+I$$

17.1) Let $R=\mathbb{Z}_6$ and let $I=(2)$. Explicitly write out the elements of R/I.

17.2) Let $R=\mathbb{Z}_9$ and let $I=(3)$. Explicitly write out the elements of R/I.

17.3) Let $R=\mathbb{Z}_3\times\mathbb{Z}_4$ and let $I=((2,3))$. Explicitly write out the elements of R/I.

17.4) Let $R=\mathbb{Z}$ and let $I=(6)$. Explicitly write out the elements of R/I. Explain how R/I is in essence $\mathbb{Z}_6$.

Definition 18 *An* ***equivalence relation*** *$\sim$ on a set R is a a subset of $R\times R$ satisfying the following three conditions:*

(i) *Reflexivity: $x\sim x$ for all $x\in R$.*

(ii) *Symmetry: If $x\sim y$, then $y\sim x$.*

(iii) *Transitivity: If $x\sim y$ and $y\sim z$, then $x\sim z$.*

Given an equivalence relation, the set $[x]=\{y\in R : y\sim x\}$ is called the ***equivalence class*** *of x.*

18.1) Given an ideal $I\subseteq R$, prove that $x+I=y+I$ if and only if $x\in y+I$.

18.2) Given an ideal $I\subseteq R$, prove that $x+I=y+I$ if and only if $x-y\in I$.

18.3) Given an ideal $I \subseteq R$, prove that

$$x + I = y + I$$

is an equivalence relation on the set of cosets of I.

18.4) Given an ideal $I \subseteq R$, prove that the operations defined on the left cosets of I are **well-defined**. That is, prove that if

$$a + I = b + I \qquad \text{and} \qquad c + I = d + I,$$

then

$$(a + I) + (c + I) = (b + I) + (d + I).$$

A similar statement should be shown for multiplication of cosets of I.

18.5) Suppose we dreamed up a new operation $\star$ on fractions:

$$\frac{a}{b} \star \frac{c}{d} = \frac{\max(a, c)}{\max(b, d)}$$

Prove that $\star$ is not well-defined over $\mathbb{Q}$.

18.6) Given a ring R and an ideal I, prove that R/I is a ring.

18.7) Let $R = \mathbb{Z}[x]$ and let $I = (x^2 + 1)$. Working in R/I, take x, square it, add 1 to it. What do you have? Is this strange?

Definition 19 *Let R be a domain and consider*

$$F(R) = \{(a, b) : a, b \in R \text{ and } b \neq 0\}$$

where

$$(a, b) \equiv (c, d) \qquad \Leftrightarrow \qquad ad = bc,$$

along with the following operations:

$$(a, b) + (c, d) = (ad + bc, bd) \qquad \text{and} \qquad (a, b) \cdot (c, d) = (ac, bd)$$

*$F(R)$ is called the **field of fractions** of R.*

19.1) Does $F(R)$ look familiar? It should!

19.2) In the definition of $F(R)$, why do we insist that R be a domain.

19.3) Prove that $\equiv$ is an equivalence relation on $F(R)$.

19.4) Prove that "addition" and "multiplication" are well-defined for $F(R)$.

19.5) Prove that $F(R)$ is a field.

19.6) Describe $F(F(R))$.

Definition 20 *A **homomorphism** of rings is a map $\varphi : R \to S$ such that for all $a, b \in R$:*

(i) $\varphi(1_R) = 1_S$.

(ii) $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$.

(iii) $\varphi(a \cdot_R b) = \varphi(a) \cdot_S \varphi(b)$.

20.1) Let $\varphi : R \to S$ be a homomorphism of rings. Prove that

$$\varphi(0) = 0.$$

20.2) Let $\varphi : R \to S$ be a homomorphism of rings. Prove that

$$\varphi(-a) = -\varphi(a).$$

20.3) Let $\varphi : R \to S$ be a homomorphism of rings. Prove that φ maps units to units and zerodivisors to zerodivisors.

20.4) Prove that the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ is a ring homomorphism.

20.5) Prove that the map $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ via

$$\varphi(x) = \begin{cases} 0 & \text{if } x \text{ is even,} \\ 1 & \text{if } x \text{ is odd,} \end{cases}$$

is a surjective homomorphism of rings.

20.6) Prove that the map $\varphi : \mathbb{Z} \to \mathbb{Z}_3$ via

$$\varphi(x) = \begin{cases} 0 & \text{if } x \equiv 0 \pmod 3, \\ 1 & \text{if } x \equiv 1 \pmod 3, \\ 2 & \text{if } x \equiv 2 \pmod 3, \end{cases}$$

is a surjective homomorphism of rings.

20.7) Prove that a homomorphism of rings $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ can be defined by setting $\varphi(1) = 1$.

20.8) Prove that the map $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ via

$$\varphi(f) = f(0)$$

is a surjective homomorphism of rings.

Definition 21 *Let $\varphi : R \to S$ be a homomorphism of rings. The **kernel** of φ is defined as*

$$\mathrm{Ker}(\varphi) = \{x \in R : \varphi(x) = 0\}.$$

*The **image** of φ is defined as*

$$\mathrm{Im}(\varphi) = \{\varphi(x) \in S : x \in R\}.$$

21.1) Given a ring homomorphism $\varphi : R \to S$, prove that φ is injective if and only if $\mathrm{Ker}(\varphi) = (0)$.

21.2) Given a ring homomorphism $\varphi : R \to S$, prove that $\mathrm{Ker}(\varphi)$ is an ideal of R.

21.3) Give an example showing that $\mathrm{Im}(\varphi)$ is not necessarily an ideal of S.

21.4) Given a ring homomorphism $\varphi : R \to S$, prove that $\mathrm{Im}(\varphi)$ is a ring.

21.5) Let R be a nonzero ring. Prove that the following are equivalent:

(i) R is a field.

(ii) The only ideals in R are (0) and (1).

(iii) Every homomorphism of R into a nonzero ring S is injective.

21.6) Let R be a ring of characteristic n. Prove that the map $\varphi : \mathbb{Z} \to R$ defined by

$$\varphi(x) = \begin{cases} \underbrace{1 + \cdots + 1}_{x \text{ times}} & \text{if } x > 0, \\ 0 & \text{if } x = 0, \\ \underbrace{-1 - \cdots - 1}_{-x \text{ times}} & \text{if } x < 0. \end{cases}$$

is a homomorphism of rings. Compute $\mathrm{Ker}(\varphi)$ for relevant and reveling values of n.

21.7*) Determine the number of ring homomorphisms between $\mathbb{Z}_n$ and $\mathbb{Z}_m$.

Definition 22 *An **isomorphism** of rings is a bijective homomorphism of rings. We say two rings R and S are **isomorphic** if there is an isomorphism between them. In this case we write $R \simeq S$.*

22.1) Prove that $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

22.2) Prove that $\mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$.

22.3) Prove or disprove that $\mathbb{Z}_3 \times \mathbb{Z}_6 \simeq \mathbb{Z}_{18}$.

22.4*) Make a conjecture about when $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{m \cdot n}$. Can you prove your conjecture? Can you further state a "simpler" ring that is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$? Can you prove this?

22.5) Prove that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

22.6) Given an injective ring homomorphism $\varphi : R \to S$, prove that $\mathrm{Im}(\varphi)$ is a ring that is isomorphic to R.

22.7) Prove that if F is a field and $\varphi : F \to R$ is a surjective homomorphism of rings, then $F \simeq R$.

22.8) Given a domain R, prove that the set $\{(a,1) : a \in R\}$ is a subring of $F(R)$, see (19), that is isomorphic to R.

22.9) Given a domain R, prove that $F(F(R)) \simeq F(R)$, see (19). Use this isomorphism to explain why

$$\frac{a/b}{c/b} = \frac{a}{c}.$$

Theorem 23 (First Isomorphism Theorem) *If $\varphi : R \to S$ is a homomorphism of rings, then*

$$R/\operatorname{Ker}(\varphi) \simeq \operatorname{Im}(\varphi).$$

Sketch of Proof Let $\varphi : R \to S$ be a homomorphism of rings.

(i) Define $\theta : R/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ via

$$a + \operatorname{Ker}(\varphi) \mapsto \varphi(a).$$

(ii) Prove that θ is well-defined.

(iii) Prove that θ is a homomorphism.

(iv) Prove that θ is bijective.

Explain how we have just proved the First Isomorphism Theorem. ■

23.1) Prove that $\mathbb{Z}_n \simeq \mathbb{Z}/(n)$. Carefully explain the distinction between $\mathbb{Z}_n$ and $\mathbb{Z}/(n)$.

23.2) Given $a, b, c, d, m \in \mathbb{Z}$, prove that if

$$a \equiv b \pmod{m} \qquad \text{and} \qquad c \equiv d \pmod{m}$$

then

$$(a + c) \equiv (b + d) \pmod{m} \qquad \text{and} \qquad (a \cdot c) \equiv (b \cdot d) \pmod{m}.$$

Explain how we have in fact already done this, see (18.4).

23.3) Explain what a GCD of two polynomials is. Hint, see the definition.

23.4) Explain how to perform the Euclidean Algorithm in $F[x]$ where F is a field. Give some relevant and revealing examples.

23.5) Prove Euclid's Lemma (all three forms) for polynomials whose coefficients are in a field. See (12.4), (12.5), and (12.6).

23.6) Do any of the forms of Euclid's Lemma hold in $\mathbb{Z}[x]$?

23.7) Let $F[x]$ be a polynomial ring over a field. Prove that $F[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible, see (14.6).

23.8) Prove that $\mathbb{R}[x]/(x^2+1)$ is isomorphic to $\mathbb{C}$.

23.9) Prove that $\mathbb{Q}[x]/(x^2-2)$ is isomorphic to $\mathbb{Q}(\sqrt{2})$.

23.10) Prove that $F = \mathbb{Z}_2[x]/(x^2+x+1)$ is a finite field. What is the order of F? See (2.5).

23.11) Prove that $F = \mathbb{Z}_2[x]/(x^3+x+1)$ is a finite field. What is the order of F? See (2.5).

Chapter 4

Solving Equations

Theorem 24 (Fermat's Little Theorem) *Let $a \in \mathbb{Z}$ and let p be a prime. Then p divides $a^p - a$.*

Sketch of Proof Proceed by induction on $|a|$ and use (7.2). Hint, start with $a = 0$. ■

24.1) Explain how Fermat's Little Theorem could be restated as: If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. Compare this with (5.7) and (5.8).

24.2) Compute the following:

(i) $3^{14} \pmod 7$

(ii) $3^{98} \pmod 7$

(iii) $3^{100} \pmod{11}$

24.3) Give two different methods for finding $2^{999} \pmod 5$, one using Fermat's Little Theorem and the other using basic problem solving methods.

Definition 25 *Let $\phi(n)$ be defined to be the number of units of $\mathbb{Z}_n$. This is sometimes written as:*

$$\phi(n) = |\mathbb{Z}_n^*| \qquad \text{or} \qquad \phi(n) = |U_n|$$

The function ϕ is called the ***Euler ϕ-function****.*

25.1) Give a completely elementary description of the Euler ϕ-function.

25.2) Try to solve (21.7).

25.3) Compute $\phi(p)$ when p is prime and prove that your answer is correct.

25.4) Compute $\phi(p^n)$ when p is prime and prove that your answer is correct.

Theorem 25.5 *Let $m, n \in \mathbb{N}$ with $(m, n) = 1$, then*

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

Sketch of Proof Consider the following array of natural numbers:

$$\begin{array}{ccccccc} 1 & 2 & \cdots & \ell & \cdots & m \\ m+1 & m+2 & \cdots & m+\ell & \cdots & 2m \\ 2m+1 & 2m+2 & \cdots & 2m+\ell & \cdots & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+\ell & \cdots & nm \end{array}$$

(i) Explain why every entry in a given column is congruent to the same element modulo m.

(ii) Explain why each column contains a different element modulo m. Also explain why each element of $\mathbb{Z}_m$ is accounted for in each row.

(iii) Explain why

$$im + r \equiv jm + r \pmod{n} \qquad \Rightarrow \qquad i \equiv j \pmod{n}.$$

Hint, use Euclid's Lemma.

(iv) Explain why every entry in a given column is distinct modulo n. Also explain why each element of $\mathbb{Z}_n$ is accounted for in each column.

Finish the proof of the above theorem. ■

25.6) Given any natural number $n \in \mathbb{N}$, explain how to compute $\phi(n)$ and give a formula.

Theorem 25.7 (Chinese Remainder Theorem) *Let $m, n \in \mathbb{N}$ with $(m, n) = 1$. Then given $y, z \in \mathbb{Z}$ there is a unique integer x between 1 and mn satisfying*

$$x \equiv y \pmod{m} \qquad \text{and} \qquad x \equiv z \pmod{n}.$$

Sketch of Proof Use the idea from (25.5). ■

25.8) Given two integers m and n such that $(m, n) = 1$, prove that

$$\mathbb{Z}/(mn) \simeq \mathbb{Z}/(m) \times \mathbb{Z}/(n),$$

see (22.4). Hints:

(i) Define a map $\varphi : \mathbb{Z} \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ via

$$x \mapsto (x + (m), x + (n))$$

(ii) Prove φ is a homomorphism of rings.

(iii) Prove that φ is surjective.

(iv) Compute $\mathrm{Ker}(\varphi)$.

(v) See (12.14).

Use the First Isomorphism Theorem (23) to complete the proof.

25.9) Explain how the result of the above exercise **is** the Chinese Remainder Theorem in disguise.

Theorem 26 (Descartes' Factor Theorem) *If α is a root of a nonzero polynomial $f(x)$ whose coefficients are in a field, then $(x-\alpha)$ is a factor of $f(x)$.*

Sketch of Proof Use the Division Theorem for polynomials, see (15.2). ■

26.1) We will prove that a nonzero polynomial of degree n over a field has at most n roots via induction on n.

(i) Prove the theorem when $n = 0$.

(ii) Now consider the case when the degree of the polynomial is positive. How many roots could this polynomial have? Zero? One? More?

(iii) Finish this proof.

Definition *Letting F be a field, define the **formal derivative** of a polynomial $f(x) \in F[x]$ as follows:*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$
$$f'(x) = n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1}x^{n-2} + \cdots + 2 \cdot a_2 x + a_1$$

26.2) Prove the product rule for formal derivatives.

26.3) Prove that $f(x)$ and its formal derivative $f'(x)$ have a common root in F if and only it is a **multiple root** of $f(x)$.

26.4) Let $f(x)$ be a polynomial over a field F whose derivative is 0. Prove that if F has characteristic 0, then $f(x)$ is a constant polynomial. What can one say when F has positive characteristic p?

26.5) Derive the quadratic formula.

26.6) Explain why one might say the complex numbers **are not** required for "solving" quadratic equations.

26.7) Explain how to solve cubic equations.

26.8) Explain why complex numbers **are** required for solving cubic equations.

Theorem 26.9* (Fundamental Theorem of Algebra) *Every nonconstant polynomial in $\mathbb{C}[x]$ has at least one root $z \in \mathbb{C}$.*

26.10) Prove that a polynomial of positive degree n in $\mathbb{C}[x]$ has exactly n roots in $\mathbb{C}$.

26.11) Show that every polynomial of positive degree in $\mathbb{R}[x]$ can be factored as a product of polynomials in $\mathbb{R}[x]$ each with degrees 1 or 2.

Definition 27 *An element α is said to be **algebraic** over a field F if α is the root of some nonzero polynomial in $F[x]$.*

27.1) Give some relevant and revealing examples of numbers that are algebraic over fields.

27.2) Prove that the sum, $c + \alpha$, and the product, $c\alpha$, of a rational number c and and algebraic number α are algebraic numbers over $\mathbb{Q}$.

Definition *If α is algebraic over a field F, then a nonzero polynomial of least degree having α as a root is called a **minimal polynomial** for α.*

27.3) Explain why every element that is algebraic over a field has a minimal polynomial.

27.4) Prove that if α is algebraic over a field F, then a polynomial $m(x)$ is minimal polynomial for α if and only if $m(\alpha) = 0$ and $m(x)$ is irreducible.

27.5) Prove that if α is algebraic over a field F, then a minimal polynomial for α divides every polynomial in $F[x]$ having α as a root.

27.6) Prove that if α is algebraic over a field F, then two minimal polynomials differ by a constant factor.

27.7) Find minimal polynomials for the following elements and fields:

(i) $\sqrt{2}$ over $\mathbb{Q}$

(ii) i over $\mathbb{Q}$

(iii) $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$

(iv) $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$

(v) $i\sqrt{2}$ over $\mathbb{Q}$

(vi) $i\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$

Theorem 27.8 *Given a field F and an element α algebraic over F with some minimal polynomial $m(x) \in F[x]$, then*

$$F[x]/(m(x)) \simeq F(\alpha).$$

Sketch of Proof Consider the map $\varphi : F[x]/(m(x)) \to F(\alpha)$ via

$$f(x) + (m(x)) \mapsto f(\alpha).$$

(i) Construct a homomorphism $\varphi : F[x] \to F[\alpha]$.

(ii) Explain why φ is surjective.

(iii) Compute $\text{Ker}(\varphi)$.

(iv) Use the First Isomorphism Theorem (23).

(v) Explain why $F[x]/(m(x))$ is a field and why $F[\alpha]$ is a field.

(vi) Explain why $F[\alpha] = F(\alpha)$.

Explain how we have just proved the theorem. ■

Definition 28 *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

*be a polynomial in $\mathbb{Z}[x]$. The **content** of f, denoted by $c(f)$ is the GCD of the coefficients of f.*

28.1) Given $f(x) \in \mathbb{Q}[x]$, prove that there exists $d \in \mathbb{Z}$ such that $c(d \cdot f(x)) = 1$.

28.2) Prove that if $f, g \in \mathbb{Z}[x]$, then

$$c(fg) = c(f) \cdot c(g).$$

Theorem 28.3 (Gauss' Lemma) *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ with $c(f) = 1$. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Sketch of Proof Prove the contrapositive of the statement and clear denominators when necessary. ■

28.4) Prove that if a polynomial factors in $\mathbb{Z}[x]$, then it factors in $\mathbb{Z}_p[x]$ for some prime p. Is the converse true? Give a proof or counterexample.

28.5) Prove a polynomial that factors in $\mathbb{Z}[x]$ also factors in $\mathbb{Z}_p[x]$ if its degree in $\mathbb{Z}[x]$ is equal to its degree in $\mathbb{Z}_p[x]$. Explain why the condition on the degree of the polynomial is necessary. Is the converse true? Give a proof or counterexample.

28.6) Prove that if a polynomial is irreducible in $\mathbb{Z}_p[x]$, then it is irreducible in $\mathbb{Z}[x]$.

28.7) Consider a polynomial $f(x) \in \mathbb{Z}[x]$ and a prime p. Prove that if the image of $f(x)$ in $\mathbb{Z}_p[x]$ (call it $\overline{f}(x)$) is irreducible and $\deg(\overline{f}) = \deg(f)$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Theorem 28.8 *The ring $\mathbb{Z}[x]$ is a UFD.*

Sketch of Proof Explain why $\mathbb{Q}[x]$ is a UFD and use Gauss' Lemma. ■

28.9) Prove that there are infinitely many irreducible (prime) numbers in $\mathbb{N}$.

28.10) Let F be a finite field. Prove that there is a polynomial of positive degree in $F[x]$ with no roots in F.

28.11) Prove there are an infinite number of irreducible polynomials in $F[x]$ where F is any field.

28.12) Let F be a field with $\alpha \in F$. Prove that $f(x) \in F[x]$ is irreducible if and only if the polynomial $g(x) = f(x + \alpha)$ is also irreducible.

28.13) Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducible polynomials.

(i) $x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

(ii) $x^3 + x + 1$ in $\mathbb{Z}_3[x]$.

(iii) $x^4 + 1$ in $\mathbb{Z}_5[x]$.

(iv) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$

(v) $x^4 + 10x + 1$ in $\mathbb{Z}[x]$.

(vi) $x^4 + 2x^2 + 1$ in $\mathbb{Z}[x]$.

28.14) Find all irreducible polynomials of degree less than 5 in $\mathbb{Z}_2[x]$.

28.15) How many irreducible quadratic polynomials are there over a finite field of n elements?

Theorem 29 (DeMoivre's Theorem) *Let α be any nonzero complex number. Then the equation*

$$x^n - \alpha = 0$$

has exactly n distinct roots, all of which are complex numbers.

Sketch of Proof We will give a direct proof of DeMoivre's Theorem *without* appealing to the Fundamental Theorem of Algebra.

(i) Prove that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.

(ii) Prove that any complex number $a + bi$ can be expressed as $Re^{i\theta}$ where $R \in \mathbb{R}$ and $\theta \in [0, 2\pi)$.

(iii) Explain why if $\alpha = R(\cos(\theta) + i\sin(\theta))$, then

$$\sqrt[n]{R} \cdot e^{\frac{i(\theta+2k\pi)}{n}}$$

is a root of $x^n - \alpha$.

(iv) Plot the roots on the unit circle, how many are there?

Explain how we have proved the theorem. ■

Definition *For $n \in \mathbb{N}$, let*

$$\zeta_n = e^{2\pi i/n}$$

*In this case we call ζ_n^k an **nth-root of unity**, where $k \in \mathbb{N}$.*

29.1) Prove that $\zeta_n^k \overline{\zeta_n^k} = 1$, where $\overline{\zeta_n^k}$ is the complex conjugate of ζ_n^k. Explain what this means geometrically.

29.2) Prove that the set

$$K_n = \{\zeta_n^k = e^{2k\pi i/n} : k \in \mathbb{N}\}$$

is a cyclic group under multiplication. Further prove that $K_n \simeq \mathbb{Z}_n$ as groups.

29.3) If $n = 2m$, prove that

$$x^n - 1 = (x-1)(x+1)q_1(x) \cdots q_{m-1}(x)$$

where $q_i(x)$ are distinct irreducible polynomials in $\mathbb{R}[x]$. Hint, see (26.11).

29.4) If $n = 2m + 1$, prove that

$$x^n - 1 = (x-1)q_1(x) \cdots q_m(x)$$

where $q_i(x)$ are distinct irreducible polynomials in $\mathbb{R}[x]$. Hint, see (26.11).

Definition *A number ζ is called a **primitive** nth root of unity if*

$$\zeta^n = 1 \qquad \text{and} \qquad \zeta^m \neq 1$$

for all $m < n$ where $m, n \in \mathbb{N}$.

Theorem 29.5 *A number ζ_n^k, where $1 \leqslant k \leqslant n$, is a primitive nth root of unity if and only if $(k, n) = 1$.*

Sketch of Proof ($\Rightarrow$) Seek a contradiction supposing that ζ_n^k is a primitive nth root of unity and that $(k, n) \neq 1$.

($\Leftarrow$) Seek a contradiction supposing $(k, n) = 1$ and ζ_n^k is not a primitive nth root of unity. Use the fact that the order of ζ_n in K_n is n and Euclid's Lemma (12.5). ■

29.6) Prove that given a prime $p \nmid n$, the primitive nth roots of unity are given by

$$\{\zeta_n^{kp} : 1 \leqslant k \leqslant n\}.$$

29.7) Prove that there are exactly $\phi(n)$ primitive roots of unity in $\mathbb{C}$.

Definition 30 *The nth **cyclotomic polynomial** is defined as:*

$$\Phi_n(x) = \prod_{\substack{(k,n)=1 \\ k<n}} (x - \zeta_n^k)$$

30.1) What is the degree of $\Phi_n(x)$?

30.2) Carefully explain each step shown below:

$$\begin{aligned} x^n - 1 &= \prod_{k=1}^{n} (x - \zeta_n^k) \\ &= \prod_{d|n} \prod_{\substack{(k,d)=1 \\ \zeta_d^k \in K_n}} (x - \zeta_d^k) \\ &= \prod_{d|n} \Phi_d(x). \end{aligned}$$

Corollary *The upshot of the above exercise is that*

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n} \Phi_d(x)}$$

30.3) Given a prime p, compute $\Phi_p(x)$.

30.4) Compute Φ_n for $n = 1, \ldots, 10$.

30.5) Prove that

$$n = \sum_{d|n} \phi(d).$$

Theorem 30.6 *The nth cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ for all $n \in \mathbb{N}$.*

Sketch of Proof Proceed by induction on n.

(i) Check the case when $n = 1$.

(ii) Now suppose our statement holds for all values less than n.

(iii) Noting that

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x).$$

Hence $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$ divides $x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$. Explain why this is also true in $\mathbb{Q}[x]$. Big hint, see the Division Theorem for polynomials, see (15.2). Use this theorem in $\mathbb{Q}(\zeta_n)[x]$ and $\mathbb{Q}[x]$ utilizing uniqueness!

Explain how to finish the proof. Hint, use (28). ■

Theorem 30.7 *The nth cyclotomic polynomial $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ for all $n \in \mathbb{N}$.*

Sketch of Proof Seeking a contradiction, suppose that $\Phi_n(x)$ is not irreducible.

(i) Explain why we may assume that $\Phi_n(x)$ is reducible in $\mathbb{Z}[x]$.

(ii) Explain why we may assume that $\Phi_n(x) = f(x) \cdot g(x)$ where $f(x)$ and $g(x)$ are monic polynomials in $\mathbb{Z}[x]$ with

$$\deg(f) < \phi(n) \qquad \text{and} \qquad \deg(g) < \phi(n).$$

Hint, use (28).

(iii) Explain why we may assume that f is a minimal polynomial for ζ_n.

Now we claim that given a prime $p \nmid n$, ζ_n^p is also a root of $f(x)$. Further seek another contradiction, and suppose that ζ_n^p is not a root of $f(x)$.

(i) Explain why ζ_n^p is a root of $g(x)$.

(ii) Explain why $f(x) | g(x^p)$ and write $g(x^p) = f(x) \cdot h(x)$, where $h(x) \in \mathbb{Q}[x]$.

(iii) Explain why we may conclude that $h(x)$ is a monic polynomial $\mathbb{Z}[x]$, use (28).

(iv) Reduce the equation $g(x^p) = f(x) \cdot h(x)$ modulo p, writing the image of the polynomials f, g, and h as $\overline{f}$, $\overline{g}$, and $\overline{h}$:

$$\overline{g}(x^p) = \overline{f}(x) \cdot \overline{h}(x)$$

(v) Explain how to use the Freshman Binomial Theorem (7.2), or Fermat's Little Theorem (24), to conclude that

$$\overline{g}(x)^p = \overline{f}(x) \cdot \overline{h}(x)$$

(vi) Explain how the fact that $\mathbb{Z}_p[x]$ is a UFD allows us to conclude that $\overline{f}$ and $\overline{g}$ have a common factor.

(vii) Explain why we must conclude that $x^n - 1$ has a multiple root modulo p. Further explain why $\overline{f}$ and $\overline{g}$ both have x as a factor, see (4). Explain why this is a contradiction.

Thus we conclude that ζ_n^p is a root of $f(x)$. Since this argument will work for any prime p with $p \nmid n$, we can show that every primitive nth root of unity is a root of f, see (29.6). This will show that $\Phi_n(x) = f$, and is hence irreducible. ■

References and Further Reading

[1] D.M. Burton. *Elementary Number Theory*. Allyn and Bacon Inc, 1976.

[2] A. Clark. *Elements of Abstract Algebra*. Dover, 1984.

[3] D.S. Dummit and R.M. Foote. *Abstract Algebra*. John Wiley & Sons Inc, 2004.

[4] J.A. Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin Company, 1998.

[5] C.C. Pinter. *Book of Abstract Algebra*. McGraw-Hill Companies, 1989.

[6] R. Solomon. *Abstract Algebra*. Brooks/Cole, 2003.

Index